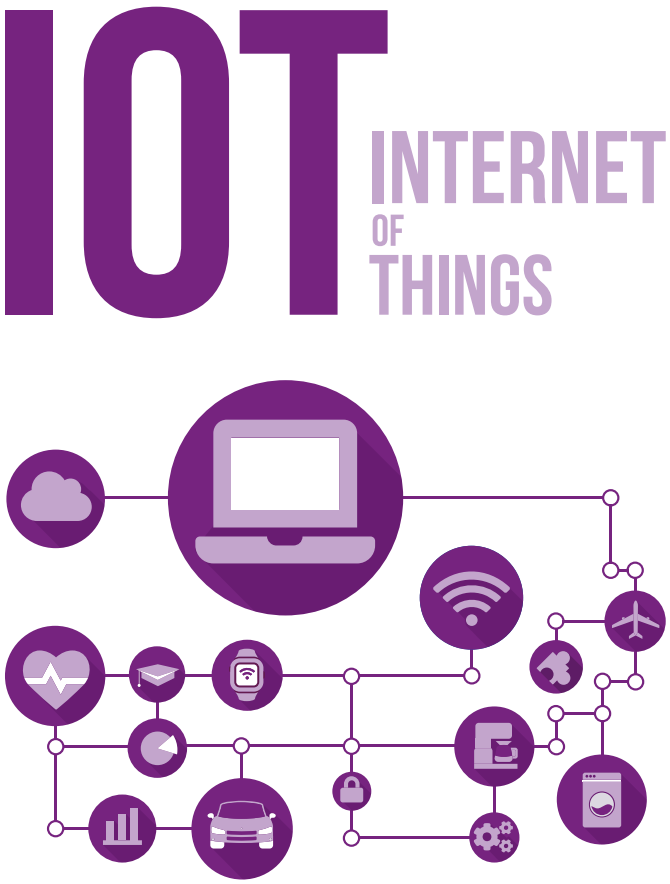
Entrust nShield HSMs enable the root of trust in the manufacture and operation of IoT devices

Bringing trust to the Internet of Things

HIGHLIGHTS

- Establishes a root of trust for device credentialing, authentication, and data protection
- Provides validation of authenticity and integrity of device software/firmware updates
- Utilizes certified hardware security modules (HSMs) to protect and manage all sensitive public key infrastructure (PKI) certificate signing keys
- Interoperates with leading Internet of Things (IoT) application vendors and backed by professional services
- Delivers complete solution from device credentialing to lifecycle management/ validation



LEARN MORE AT ENTRUST.COM/HSM

Enabling the root of trust in the manufacture and operation of IoT devices

The ability to distribute connected devices across a geographically-dispersed network provides organizations valuable functionality and opportunities for additional revenue. However, the IoT also presents considerable security risks and challenges for organizations. Specifically:

- Attackers impersonating a trusted device could conduct man-in-the-middle or other attacks
- Attacks on unsecured devices could expose protected content or enable access to other connected systems
- Without a root of trust, communications could be compromised, delivered incompletely, or lost
- The privacy and integrity of data stored on, and transmitted with, unsecured devices cannot be guaranteed

According to the 2020 Ponemon PKI and IoT Trends Study, in the next two years an average of 43% of IoT devices will rely primarily on digital certificates for identification and authentication. With billions of devices being deployed, demand for PKIs to issue digital certificates is rapidly increasing. Once devices are deployed, operators must also ensure that code updates sent to devices are authorized and authentic, as software that has been altered or corrupted can expose the entire organization once it executes.

Protecting IoT data collected from dispersed endpoints presents a myriad of challenges, but one thing is certain: if you can't trust the data, there's no point in collecting, analyzing and making business decisions based on it. Entrust's solutions for IoT focus on the fundamentals of both device security and data protection to provide a root of trust for the entire ecosystems.

To securely participate in the IoT, each connected device needs a unique identification – even before it has an IP address. This digital credential establishes the root of trust for the device's entire lifecycle, from initial design to deployment to retirement.

Entrust's nShield® HSMs, combined with supporting security applications from our nFinity technology partners, enable manufacturers to provide each device a unique ID using the strongest cryptographic processing, key protection, and key management available. A digital certificate is injected into each device to enable:

- Authentication of each device introduced to the organization's architecture
- Verification of the integrity of the operating system and applications on the device
- Secure communications between devices, gateway, and cloud
- Authorized software and firmware updates, based on approved code

All nShield HSMs feature our market-leading Security World key management architecture—proven technology that protects application keys within the safe confines of the HSM, yet allows them to be managed in a straightforward and convenient manner.

PKI Support

The IoT requires a secure and scalable solution for managing and protecting digital certificates. Based on the knowledge gained during hundreds of PKI deployments, we have the expertise to help you build a PKI that meets your needs, regardless of scale or complexity. By securing the process of issuing

Enabling the root of trust in the manufacture and operation of IoT devices

certificates and proactively managing signing keys, you prevent their loss or theft, thereby creating a high-assurance foundation for digital security. Whether you work with one of our industry-leading PKI partners or tap into our nShield professional services for support, nShield HSMs provide an independently certified, tamper-resistant devices to secure some of your most sensitive keys and business processes in the organization—a widely recognized PKI best practice.

> Entrust's proven track record of delivering best-in-class cryptographic hardware security and key management will benefit our developers and the larger ecosystem by enabling a new generation of IoT products and applications to enter the market with enhanced privacy and security features critical for the broad array of products and services."
>
> **Curtis Sasaki, VP Ecosystems, Samsung Electronics**

Fast, efficient cryptography

Entrust nShield HSMs supports all major cryptographic algorithms and offers the world's fastest support for elliptic curve cryptography (ECC). Given the limited processing power available with many small connected devices, ECC provides a strong and efficient alternative to traditional algorithms. Custom algorithms are also supported, executing them within the protected environment of the HSM using Entrust's unique CodeSafe capability.

Securing offshore production

When outsourcing production, either in part or completely, organizations need assurance that manufacturing is completed according to project specifications. A combination of Entrust HSMs and credentialing software allows manufacturers to control the number of units produced as well as what code is built into each, even in a geographically-dispersed supply chain. This prevents unauthorized production runs and the introduction of unapproved code.

Code signing

The Entrust code signing solution helps software producers of all types implement highly secure and efficient code signing processes that protect their organizations from risks associated with software tampering. Combining tamper-resistant nShield HSMs with professional services, the Entrust code signing solution is backed by our extensive expertise in code signing best practices and standards of due care. Our proven HSMs provide tamper-resistant, certified protection for private code signing keys and a secure platform to perform critical digital signature processes.

Device-level security and data protection

The combination of device-level protection delivered by Entrust nShield HSMs provide high assurance security to enterprise and cloud-based deployments where IoT data is stored, aggregated and analyzed.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com